

# **ILLEGAL ETHNOGRAPHIES**

**A Guide to navigating  
Ethics and Data Protection  
in Ethnographic Research  
in illegal, or less democratic,  
fieldsites.**

By

Lida Farakouki

Mowgli Legein

Tabea Pawar

# **CONTENTS**

- ⇒ Introduction
- ⇒ Disclaimer
- ⇒ Participant Observation
- ⇒ Data Protection
- ⇒ Confidentiality and Anonymity

Since anthropology is the study of human cultures and practices, as an anthropologist you might consider doing research about a group or community that is involved in some form of not-so-legal activity.

Whether it may be illegal migrants, substance abusers, radical activists, or other socio-politically vulnerable or oppressed groups, some of the most relevant ethnographic insights might involve witnessing or even taking part in certain illegal activities.

To help navigate these situations, we have constructed a guide to consider whilst finding the means to protect yourself and those researched in trickier ethnographic fieldsites.

# **DISCLAIMER**

Please do note this is a guide compiled by students whose closest „experience“ to such dangerous fields is restricted to having read and consulted published ethnographies, where the contents of this zine is largely drawn from.

We simply hope this compilation draws attention to aspects of your and your participants safety to consider and consult, both before and while embarking on your fieldwork.

# Participant Observation

When dealing with sensitive and potentially dangerous situations, the first step of a researcher is to critically reflect on what could potentially threaten their own safely...

**To what extent do you want to get involved in your field ?**



Anthropological research is often characterized by **participant observation**; a method in which the researcher comes to spend a significant amount of time in the field taking notes, interacting with research participants, **and taking part in their activities**.

SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS

**In any research, the ethnographer would have to decide to what extent they would want to get **involved** in their field.**

While being just an observer might enable more **critical distance**, it is generally advised to try and part take as much as possible in events taking place to not only **create a relationship with your participant(s)**, but to fully access that **insider's worldview**.

SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS

When conducting research in situations that involve illegal activities, the choice to participate has higher stakes.

Participation could result in losing the protection of your institution, getting banned from your fieldsite, fined or even facing jail time.

On the other hand, participation would help your participants develop trust in you and thus allow you to gain valuable insights by becoming **“one of them”**.

- ⇒ **Consider the risks associated to your participation.**
- ⇒ **Make a concrete distinction for yourself; a boundary you will ideally avoid crossing.**
- ⇒ **Think about how to mitigate consequences if you do find yourself crossing your, your institutions' or the States boundaries.**

# To what extent could being open about your role as a researcher endanger you ?



While getting **informed consent** from the researched population is one of the main **ethical principles of the American Anthropology Association**, some anthropologists argue that in certain circumstances, disclosing one's identity threatens not only their research but their own lives.

Charlotte Thomas Hébert (2019) explains that while she was conducting research about **non violent direct action** and **civil disobedience** in the USA, she would not disclose her position as a researcher during the **demonstrations**.

She believed being present during those demonstrations was key in understanding her field, but she could not risk being **arrested** since she was not an american citizen and risked getting **deported** if the government came to know she was involved in illegal activities.



Similarly, **Philippe Bourgois** (2003) also tried to walk the thin line between witnessing illegal activities and participating in them.

He conducted research about **crack houses** in **East Harlem**, after moving to the neighborhood himself and becoming friends with some of the **leaders of the drug network**.

While his main participants were aware of his role as a researcher, he explains he didn't tell most of the other members of the community; they were already **highly suspicious** of him and he justifies it would have **compromised his research**

# Data Protection

Having gained insider access to a **highly sensitive research environment** or community, it is your **responsibility** as a researcher **to take precautionary measures** regarding the safekeeping of your information...

## What threats could your data face?

SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS

Condensed from the Electronic Frontier Foundation project, 'Surveillance Self-Defense' (available at: <https://ssd.eff.org/en>), here are...

### *4 questions to ask yourself before (and during) your work in the field.*

- ⇒ What about your research could be of value to someone else?
- ⇒ Who, or what, might be interested in your data?
- ⇒ What are potential consequences if your data is accessed by someone unauthorised?
- ⇒ Are you doing what you can to limit access to your information?

SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS



A fool-proof strategy is arguably to keep valuable information either in analogue form, such as a notebook, or offline, such as in an external encrypted hard-drive.


However, in situations such as those faced by **Seth M. Holmes** (2013) whilst he accompanied his participants, migrant farm workers, in **illegally crossing the border** from Mexico to Arizona (and was **jailed** with them for this), carrying around a valuable object that does not have a back-up is not ideal. Neither in terms of data safety, nor efficiency in the field.

Thus, below and on the next page are several non-profit sources which can help you set up the optimal data defence toolbox to help protect your information, which is ultimately that of your participants to whom you have a certain duty of care.



**SSD.EFF.ORG**

⇒ Comprehensive website containing step-by-step guides for installing protection across various devices and helping visualise potential risks in the first place.


 [securityinabox.org/en/](https://securityinabox.org/en/)

**security in-a-box**

digital security tools and tactics

⇒ Tactic toolboxes to help improve your digital security across interfaces, platforms and systems.



 [defendourmovements.org/resources/](https://defendourmovements.org/resources/)


## DEFEND OUR MOVEMENTS

DIGITAL SELF-DEFENSE KNOWLEDGEBASE

⇒ Part of the privacy and power in technology movements in the USA, Defend Our Movements is a pool of resources for activists and journalists who may seek to protect themselves and their digital data from prying eyes.

⇒ Smaller, everyday steps one can take to minimise their data footprint, which is useful for privacy in both personal life but also the field.



 [datadetoxkit.org/en/home/](https://datadetoxkit.org/en/home/)

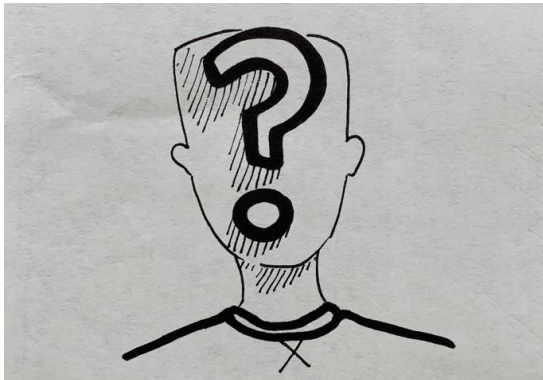
It would be impossible to erase all risks concerning data protection, but depending on the situation, an attempt to minimize the likelihood, severity and damage of potential data breaches is crucial.

**Being alert and aware is crucial.**



# Confidentiality & Anonymity

As essentially *all* anthropological or social research ethical guidelines will tell you, we have a certain responsibility towards our research participants; to not only **respect them and their boundaries** within our research, but to also **protect them from any unintended consequences** being involved with our research might bring. Thus comes the principle of **maintaining information confidentiality** and **participant anonymity**.



**Protecting the identity of the researched reduces the risk of them facing consequences of your behalf.**

## **Step #1: Establish protocols on how you will keep your participant information confidential**

- ⇒ Create identifier codes for participants: reduce the direct risk of identification by assigning neutral (i.e. numerical) codes to each participant. This is especially important in the case of sustained contact.
- ⇒ Store participant contact information separately from associated transcripts and notes, in a secure location: the more obstacles to gaining complete insight to your data and participants, the better. Although do keep in mind the time and resources required to set these in place.
- ⇒ Take the notion of data protection, elaborated on the previous pages, seriously.



## **Step #2: Establish protocols on how you will anonymise your participants [incl. the fieldsite!]**

- ⇒ Here it is important to consider what form your research is going to take; written dissemination will face other anonymisation processes as compared to visual or audio forms of publication.
- ⇒ If deemed appropriate, ask the participants what they feel comfortable with: you can involve your participants in the process. They are after all experts of the field you seek to understand and anonymise.

## Methods for anonymising sources in WRITTEN research dissemination:

- ⇒ **Pseudonyms:** assigning a pseudonym entails giving your participants a different name to hide their identity, right from the point of taking fieldnotes to the point of publication, where it is assumed you represent your participants in some form through your work. **A pseudonym is unrelated to any real names of people or places encountered during research.**
- ⇒ **Fabrication:** taking into account the details in conversation which may give away information which could help identify people or a place, **Markham** (2012) elaborated on how **data fabrication can be ethically implemented** to produce snippets of data that represent reality to the reader, but do not entail verbatim reality which could pose threat to participant anonymity. Although Markham speaks in the context of digital ethnography, her argument for fabrication of data through authority and credibility of the ethnographer stands across contexts.

## Method for anonymising sources in AUDIO-VISUAL research dissemination:

- ⇒ Playing with light: filming with backlight or silhouettes masks the participants visual identity creatively.
- ⇒ Pixelating faces in post-production: keep in mind the digital security of your data in production and storage.
- ⇒ Warping voices: pitch changes can theoretically be quite easily reversed, which is why sound warping may prove more efficient.

# Conclusion

As we have tried to emulate over the course of this zine, conducting research in communities that involve illegal activities or working with particularly oppressed or vulnerable groups requires a particular set of ethical considerations.

Firstly, the researcher has to take precautions to protect themselves, by considering the extent of institutional protections and the local laws of their field, but also by reflecting on the extent to which they can participate safely in this specific community.

Additionally, the ethnographer must take the safety of the participants into consideration. The researcher must therefore have an infallible data risk management plan to safely store and protect collected data as well as have the necessary tools to protect participant identity.

One more summary bit for Lidas sections maybe here?

**SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS**

Conducting ethnographic research in more precarious fieldsites poses similar ethical challenges to the researcher as any ethnographic project would, except that the legal and psychological stakes, or risks, are higher.

This zine aims to show any upcoming anthropologist that there is no simple ethical protocol to apply when it comes to field work in an vulnerable/illicit site.

Therefore, despite our guide, we believe the most valuable advice would be to contact other researchers who might have past experience in a similar field or speak to a trusted gatekeeper who is accustomed to the dynamics of the field work, to gain better understanding in preparation for yours.

As Mutaru( 2018) explained about his time in Ghana, the local cultural and moral norms are very important to keep in mind when navigating sensitive and potentially dangerous ethnographic sites.

The ethical choices you make will depend on the context of your field, the legal environment and the relationships you have with your participants.

**SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS SECURITY SEAL DO NOT CROSS**

# References

## **Cited Ethnographies:**

Bourgois, P. (2003). *In search of respect : Selling crack in the barrio* (Second ed., *Structural analysis in the social sciences*).

Holmes, S.M. (2013). *Fresh fruit, broken bodies: Migrant farmworkers in the United States* (University of California Press).

## **Cited Journal Articles:**

Thomas-Hébert, Charlotte. 2019. “Conducting Sensitive Research as an Alien Ethnographer in the United States.” *American Studies Journal* 68.

Markham, Annette. 2012. “Fabrication as Ethical Practice: Qualitative Inquiry in Ambiguous Internet Contexts.” *Information, Communication & Society* 15 (3): 334–53.

Mutaru, Saibu. 2018. “Conducting Anthropological Fieldwork in Northern Ghana: Emerging Ethical Dilemmas.” *Anthropology Southern Africa* 41 (3): 185–98.

## **Other interesting links:**

<https://holistic-security.tacticaltech.org/chapters/prepare.html>

<https://exposingtheinvisible.org/en/articles/technology-is-stupid/>

<https://ourdataourselves.tacticaltech.org/projects/data-and-activism/>

<https://kit.exposingtheinvisible.org/en/how/field-research.html>

<https://kit.exposingtheinvisible.org/en/how/interviews.html>